Information Services Board Briefing Paper on Statewide Information Technology Policy Compliance

Prepared by Andy Hix, DIS/MOSTD (360) 902-3431 andyh@dis.wa.gov

Presenter
Andy Hix, DIS/MOSTD

Purpose of Appearance
To review the status of agencies' 2004 certification of compliance with IT policy and standards pertaining to Portfolio Management, Disaster Recovery/ Business Resumption, and IT Security, and to recommend action with respect to non-compliant agencies.

Previous ISB Appearance
March 18, 2004
Staff presented information on agencies' policy compliance for the August 2003 certification deadline. In response to the non-compliant agencies, the Board removed delegated authority until such time as they became compliant. The Board also asked staff to report on agency compliance for 2004 at the September 2004 Board meeting.

September 2004
Staff distributed information on the status of agency policy compliance certifications for the August 31, 2004 deadline.

November 2004
Staff distributed updated information on the status of agency policy compliance certifications.

January 2005
Staff distributed further updates to the policy compliance certification response.

Staff Recommendation to the Board
Consistent with action taken last year, ISB staff recommends the Board remove delegated authority for information technology purchases for agencies that remain non-compliant with the ISB policy.

MOSTD will notify the non-compliant agencies of the removal of delegated authority. Staff also recommends that by the next scheduled ISB meeting the Board require non-compliant agencies to provide a specific date that they will be compliant. Finally, staff recommends that as it did last year, the Board delegate to the Deputy Director of DIS the authority to restore agencies' delegated authority upon certification that they are in compliance with the respective ISB policies and standards.

Issues
Does removal of delegated authority function as an effective deterrent for non-compliance with ISB policies?

Yes, it appears so. While the overall numbers of non-compliant agencies have not dropped substantially from last year to this year, most of last year's delinquent agencies did become compliant within a few months of last year's Board action removing their

delegated authority. With the exception of one agency, none of the agencies that were delinquent last year are delinquent this year.

What impact does removal of delegated authority have on an agency's IT operations?

Under specifically defined circumstances agencies are delegated authority to make IT investments without first obtaining approval from the Information Services Board. Removal of delegated authority means the ISB must approve any proposed IT investment before the agency can acquire it. Portfolio Management defines investment as follows:

"For purposes of the portfolio, an investment is defined to be a specific piece of hardware/peripherals or a software application developed at agency expense or acquired from vendors, or any combination of these events, that serves current and future needs of the agency."

Therefore removal of delegated authority will not have any impact on agency projects that have already been initiated, or on ongoing IT maintenance operations. It will however, require prior board approval of any acquisition, whether it be a mainframe, a PC, or development of an application, regardless of cost.

Background
The ISB policies direct agencies to review and update their IT Portfolio, Disaster Recovery/Business Resumption Plan and IT Security Program annually. Each agency director is responsible for oversight of the agency's plans and programs and is to confirm in writing annually by August 31st that the portfolio was reviewed and updated, the Disaster Recovery/Business Resumption Plans have been reviewed, updated, and tested and the IT Security Program has been developed, reviewed and updated.

Additionally, the IT Security policy requires agencies to conduct an IT security policy and standards compliance audit once every three years. The audit is a desk review of the documented agency security processes and procedures. The audit's findings on exceptions to the policy and standards are provided only to the agency. Knowledgeable parties independent of the agency's information technology unit, such as a state auditor, must perform the audit. All agencies under the authority of the ISB were required to complete their initial compliance audit by October 6, 2003.